JO1P0364 US00

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed this Office.

出願年月日
Date of Application: ２０００年　８月２３日

出願番号
Application Number: 特願２０００－２５２８０４

出願人
Applicant(s): ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年１２月２２日

特許庁長官
Commissioner,
Patent Office 及川耕造

【書類名】　特許願
【整理番号】　0000612902
【提出日】　平成12年 8月29日
【あて先】　特許庁長官殿
【国際特許分類】　H04K 1/00
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　市村　元
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代表者】　出井　伸之
【代理人】
【識別番号】　100086841
【弁理士】
【氏名又は名称】　脇　篤夫
【代理人】
【識別番号】　100114122
【弁理士】
【氏名又は名称】　鈴木　伸夫
【手数料の表示】
【予納台帳番号】　014650
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9710074

【包括委任状番号】　0007553

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ送出装置、データ送出方法

【特許請求の範囲】

【請求項１】　主データと付加データとが配される複数のデータブロックを連続的に送出することで、一連の主データ及び上記一連の主データに係る付加データを送出するデータ送出装置において、

上記付加データを、一連の主データを構成する上記連続したデータブロックのうちでランダムに選択したデータブロックに挿入する付加データ挿入手段と、

上記付加データ挿入手段での付加データ挿入処理が行われた、連続するデータブロックに対して暗号化処理を行う暗号化手段と、

上記暗号化手段により暗号化された連続するデータブロックを送出する送出手段と、

を備えたことを特徴とするデータ送出装置。

【請求項２】　上記データブロックの一部に乱数データを挿入する乱数データ挿入手段をさらに備え、

上記暗号化手段は、上記付加データ挿入手段での付加データ挿入処理、及び上記乱数データ挿入手段での乱数データ挿入処理が行われた、連続するデータブロックに対して暗号化処理を行うことを特徴とする請求項１に記載のデータ送出装置。

【請求項３】　上記付加データ挿入手段は、暗号化されていない付加データを、ランダムに選択したデータブロックに挿入することを特徴とする請求項１に記載のデータ送出装置。

【請求項４】　上記付加データ挿入手段は、暗号化されていない付加データ、及び暗号化されている付加データを、ランダムに選択したデータブロックに挿入することを特徴とする請求項１に記載のデータ送出装置。

【請求項５】　上記乱数データ挿入手段は、データブロック内における無効データ部分に、上記乱数データを挿入することを特徴とする請求項２に記載のデータ送出装置。

【請求項６】　上記送出手段は、有線又は無線で接続された他の機器に対して上記連続したデータブロックを送出することを特徴とする請求項１に記載のデータ送出装置。

【請求項７】　上記送出手段は、上記連続したデータブロックを記録媒体に記録するデータとして送出することを特徴とする請求項１に記載のデータ送出装置。

【請求項８】　主データと付加データとが配される複数のデータブロックを連続的に送出することで、一連の主データ及び上記一連の主データに係る付加データを送出するデータ送出方法において、

上記付加データを、一連の主データを構成する上記連続したデータブロックのうちでランダムに選択したデータブロックに挿入し、

付加データ挿入処理が行われた、連続するデータブロックに対して暗号化処理を行ない、

暗号化された連続するデータブロックを送出することを特徴とするデータ送出方法。

【請求項９】　上記データブロックの一部に乱数データを挿入する乱数データ挿入処理が行われ、

上記付加データ挿入処理、及び上記乱数データ挿入処理が行われた、連続するデータブロックに対して上記暗号化処理が行なわれることを特徴とする請求項８に記載のデータ送出方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、主データ及び付加データを暗号化して送出するデータ送出装置、データ送出方法に関するものである。

【０００２】

【従来の技術】

例えば著作権保護が必要なデータ、秘密性の高いデータ、プライバシーにかかる私的データなど、外部に漏洩することが好ましくないデータの伝送に際しては

、暗号化処理が行われることが多い。

例えば図１１に或る送信装置１０１から受信装置１０２に対してデータを暗号化して伝送するモデルを示す。

【０００３】

いま、伝送しようとするデータが送信装置１０１に入力されたとすると、送信装置１０１は、まず暗号化部１１１で暗号化処理を施し、暗号化されたデータＤＴｓを生成する。

そしてそのデータＤＴｓは送信部１１２から送信出力される。

送信出力されたデータＤＴｓは例えばＩＥＥＥ１３９４バスなどの伝送路１０３により、受信装置１０２に送られることになる。

受信装置１０２では、伝送路１０３から送信されてきたデータＤＴｓを受信部１２１で受信し、復号部１２２で暗号解読処理を行うことで、元のデータを得ることができる。

【０００４】

【発明が解決しようとする課題】

このように伝送路１０３においては暗号化されたデータＤＴｓが送信されることで、仮に伝送路１０３においてデータＤＴｓが取り出されたとしても、伝送データの内容は秘密性が保たれるものとなる。

しかしながら、例えば著作権保護を目的として音楽データ等を図１１のようなシステムで伝送する場合、暗号を解読され、結果として違法なコピーが行われるおそれがある。

【０００５】

ここで、図１１に破線で示すように、何らかの手段で伝送路１０３から暗号化されたデータＤＴｓが取り出されたとする。

通常は、データＤＴｓを解析しても、元のデータ自体の内容がわからないため、暗号の解読は困難である。

ところが、元のデータの内容が明白にわかる部分としての暗号化データＤＴｓを抽出されると、その元のデータ内容と暗号化データを比較解析することで暗号化アルゴリズムが知られてしまう危険性がある。

そして暗号化アルゴリズムが解読されれば、悪意のユーザーによればその後データの違法な取り込みが容易に可能となってしまう。つまり著作権侵害となるような行為を実行可能としてしまう。

【０００６】

元のデータの内容が明白なものとしては、例えば音楽データ等と同時に伝送される付加データ内の一部が考えられる。

一般に、音楽データ、映像データ等のデジタルデータコンテンツの伝送を行う場合、音楽や映像としての主データだけでなく、各種の付加データが付加されることが行われている。

例えば音楽データでいえば、曲名、歌詞、作詞作曲者名、アーティスト名などのテキストデータや、イメージ画像、写真画像などの画像データが、付加データとして同時に伝送される。

【０００７】

これらの付加データとしては、伝送前の段階で光ディスク、ハードディスク、メモリカードなどのメディア上に、音楽データとともに既に記録されているものや、伝送時に新たに付加するものなどがある。

そして曲名、歌詞などの付加データであっても、メディア上において既に暗号化されて記録されている場合は、その付加データは上記の暗号化データＤＴｓに対して「元の内容が明白なデータ」とはならない。つまり伝送の際の暗号化部１１１での暗号化の前の段階で既に暗号化されたデータであるためである。

【０００８】

例えば伝送路１０３から暗号化データＤＴｓを抽出した悪意のユーザが、伝送されている音楽の曲名を知り、暗号化データＤＴｓのうちのその曲名データ部分を抽出して比較解析したとしても、暗号化される前の曲名データが既に暗号化されていれば、暗号化部１１１での暗号化アルゴリズムの解析はほぼ不可能となる。

【０００９】

また、画像データの場合は、画像フォーマット、圧縮方式などのデータ形式の多様性から、画像自体がわかっていても、その画像データ自体は通常わからない

。従って悪意のユーザーが画像データ部分を元にして暗号化アルゴリズムを解くことも不可能に近い。

【００１０】

ところが、暗号化部１１１での処理の前で暗号化されていない付加データがあった場合、その付加データの元のデータ内容を悪意のユーザーが予測できるものがある。

例えば音楽データの場合、伝送時にＩＳＲＣ（International Standard Recording Code）を付加することが行われる。

このＩＳＲＣは音源（楽曲）に固有に付される国際規格コードであり、各音源に対して国名、会社名、録音年、レコーディング番号などを示すコードとされる。

そして或る楽曲についてのＩＳＲＣは、例えばＣＤ等の販売に用いられる音楽カタログなどから知ることができる。

従って、伝送データにＩＳＲＣが付加データとして付加されていた場合、悪意のユーザーにとっては、それは「元の内容が明白なデータ」となり、その暗号化データＤＴｓからＩＳＲＣが付加された部分を抽出し、実際のＩＳＲＣのデータと比較解析することで、暗号化アルゴリズムが解析できる可能性が生ずる。

【００１１】

またＩＳＲＣに限らず、例えば曲名、アーティスト名、ディスク製造番号などであっても、暗号化部１１１での処理前に既に暗号化が施されているのでなければ、それらも悪意のユーザーにとって「元の内容が明白なデータ」となり、暗号化アルゴリズムの解析や、著作権侵害行為を可能としてしまう可能性がある。

【００１２】

従って、音楽データ等の著作権保護が必要なデータについて、機器間の伝送、記録媒体への記録のための伝送、或いは公衆回線等を用いた音楽配信システムにおける伝送などの広範囲の分野で、上記の危険性が内包されており、このため元の内容が明白なデータを伝送する場合でも、違法な暗号解読を防止できるような技術が求められている。

【００１３】

【課題を解決するための手段】

本発明はこのような状況に鑑みて、伝送されるデータについて、容易に暗号解読ができないようにする技術を提供するものである。

【００１４】

このため本発明では、主データと付加データとが配される複数のデータブロックを連続的に送出することで、一連の主データ及び上記一連の主データに係る付加データを送出するデータ送出装置において、上記付加データを、一連の主データを構成する上記連続したデータブロックのうちでランダムに選択したデータブロックに挿入する付加データ挿入手段と、上記付加データ挿入手段での付加データ挿入処理が行われた、連続するデータブロックに対して暗号化処理を行う暗号化手段と、上記暗号化手段により暗号化された連続するデータブロックを送出する送出手段とを備えるようにする。

例えば上記付加データ挿入手段は、暗号化されていない付加データを、ランダムに選択したデータブロックに挿入する。

或いは上記付加データ挿入手段は、暗号化されていない付加データ、及び暗号化されている付加データを、ランダムに選択したデータブロックに挿入する。

【００１５】

また、上記データブロックの一部に乱数データを挿入する乱数データ挿入手段をさらに備え、上記暗号化手段は、上記付加データ挿入手段での付加データ挿入処理、及び上記乱数データ挿入手段での乱数データ挿入処理が行われた、連続するデータブロックに対して暗号化処理を行うようにする。

また上記乱数データ挿入手段は、データブロック内における無効データ部分に、上記乱数データを挿入する。

【００１６】

またデータ送出装置は、それぞれ異なる機器としての送信装置、受信装置においてデータ伝送を行う場合の、上記送信装置として実現する。或いは、記録媒体に記録を行う記録装置における記録データの送出装置として実現されるようにする。

【００１７】

また本発明のデータ送出方法は、付加データを、一連の主データを構成する上記連続したデータブロックのうちでランダムに選択したデータブロックに挿入し、付加データ挿入処理が行われた、連続するデータブロックに対して暗号化処理を行ない、暗号化された連続するデータブロックを送出する。

また、上記データブロックの一部に乱数データを挿入する乱数データ挿入処理が行われるようにし、上記付加データ挿入処理、及び上記乱数データ挿入処理が行われた、連続するデータブロックに対して上記暗号化処理が行なわれるようにする。

【００１８】

即ち本発明では、送信の際の暗号化を行う前における連続したデータブロックに対して、付加データをランダムに選択したデータブロックに付加することで、付加データが付加される位置が連続するデータブロック内でランダムなものとなるようにする。つまり伝送されている暗号化データにおいて、「元の内容が明白なデータ」が配されている位置がわからないようにすることで、「元の内容が明白なデータ」に相当する暗号化データを抽出できないようにし、これによって暗号アルゴリズムが解読できないようにする。

またデータブロックの一部に乱数データを挿入することで、より暗号アルゴリズムの解読を困難とする。

【００１９】

【発明の実施の形態】

以下、本発明の実施の形態を次の順に説明する。

１．送信装置に本発明を採用する例

２．ＩＥＥＥ１３９４の伝送フォーマット

３．ＩＥＥＥ１３９４でオーディオパケットデータを伝送する場合の付加データのランダム挿入例

４．記録装置に本発明を採用する例

【００２０】

１．送信装置に本発明を採用する例

本発明のデータ送出装置（データ送出方法）を、送信装置に採用する実施の形態を説明する。

図１は、或る２つの機器が例えばＩＥＥＥ１３９４バスによる伝送路３により接続されている場合に、送信装置１を有する機器から受信装置２を有する機器に音楽データ等のデータＤＴ、及びデータＤＴに付随する付加データＤａ１，Ｄａ２を伝送するモデルにおいて本発明の実施の形態を示したものである。

パケット構造については後述するが、データＤＴは、例えば１ビットデジタルオーディオデータを、所定の伝送プロトコルに合致するフォーマットに基づいてパケット化（ブロック化）したものであるとする。また付加データＤａ１，Ｄａ２は、そのブロック内に含まれて伝送される。

【００２１】

１ビットデジタルオーディオデータとは、通常のＣＤ（Compact Disc）におけるオーディオデータよりも高品位なデータとして開発されたものであり、サンプリング周波数を例えばＣＤ方式における４４．１ＫＨｚの１６倍という非常に高いサンプリング周波数である２．８４２ＭＨｚとしてΔΣ変調された１ビットデータのことであり、周波数帯域はＤＣ成分～１００ＫＨｚの広範囲とされ、ダイナミックレンジはオーディオ帯域全体で１２０（ｄＢ）を実現できるデータ形式である。

なお、本例ではこのような１ビットデジタルオーディオデータをパケット化して伝送する場合を例に挙げるが、もちろん伝送されるデータ自体の形式、種別はどのようなものでもよい。

【００２２】

図示するように送信装置１は、ブロック処理部１０、ランダムデータ付加部１１，暗号化部１２、送信部１３が設けられる。

この送信装置１に対しては、伝送するデータとして、例えば光ディスク、ハー

ドディスク、メモリカード等の所要のメディアから読み出された１ビットデジタルオーディオデータとしてのデータＤＴ、及びこの主たるデータＤＴに付随して、同じくメディアから同時に読み出された付加データＤａ１が供給される。なお、この場合においてデータＤａ１はメディア上で既に暗号化されて記録されていたものとし、送信装置１に入力される時点では暗号化された付加データとなっているものとする。

また、当該１ビットデジタルオーディオデータとしてのデータＤＴの伝送に際して、さらに付加データＤａ２が伝送されるべきデータとして与えられるものとする。具体例としては付加データＤａ２はＩＳＲＣであるとする。そして、このＩＳＲＣは送信装置１に入力される時点では暗号化されていないデータである。

【００２３】

ブロック処理部１０は、データＤＴ、付加データＤａ１，Ｄａ２について、後述するＩＥＥＥ１３９４による伝送フォーマットに即したブロックとしてのデータストリームに形成する処理を行う。

具体的なブロック例は後述するが、所定のチャンネル数の１ビットデジタルオーディオデータを配したブロックが連続されることで、例えば１つの楽曲としてのデータストリームが形成される。また各ブロックには付加データＤａ１，Ｄａ２を配する領域や無効データが充填される領域が設定されている。

ここで、本例では少なくとも付加データＤａ２について、或いは付加データＤａ１，Ｄａ２について、連続するブロックのうちでランダムに選択したブロック内に配置されるようにするものである。

【００２４】

ランダムデータ付加部１１は内部に乱数発生回路を備え、送信しようとするデータＤＴ（パケットデータを構成するブロック）の所要の部分に乱数発生回路で発生させた乱数データを付加する動作を行う。

暗号化部１２は、ランダムデータ付加部１１の出力に対して所定の暗号アルゴリズムでの暗号化処理を施す。

送信部１３は暗号化部１２の出力をＩＥＥＥ１３９４バスによる伝送路３に送出する動作を行う。

【００２５】

受信装置２は、受信部２１，復号部２２、ブロックデコード部２３を備える。

受信部２１は、伝送路３から供給されるデータを受信して取り込む動作を行う。

復号部２２は、上記暗号化部１２での暗号化アルゴリズムに対応して暗号解読処理を行う部位である。

ブロックデコード部２３は、上記ランダムデータ付加部１１で付加された乱数データ部分を除去するとともに、一連のブロックデータから付加データＤａ１，Ｄａ２を抽出する。もちろん各ブロックデータから１ビットデジタルオーディオデータとしてのデータＤＴも取り出す。

【００２６】

このような送信装置１、受信装置２においてデータＤＴの伝送は次のように行われる。

パケットデータとして伝送しようとするデータＤＴ、付加データＤａ１、Ｄａ２が送信装置１に入力されたとすると、送信装置１は、まずブロック処理部１０でパケットを構成する一連のブロックデータによるデータストリームを生成する。このとき上記のように付加データＤａ２（又はＤａ１、Ｄａ２）はランダムなブロックに挿入する。

ランダムデータ付加部１１で、パケット内の所定の部位に乱数データを挿入する。具体例は後述するが、パケットデータ内の無効データ部分に乱数データを挿入することになる。

ランダムデータ付加部１１で乱数データが挿入されたデータＤＴａｄは、続いて暗号化部１２に供給され、暗号化処理が施される。

暗号化されたデータＤＴｓは、送信部１３に供給され、送信部１３から伝送路３に対して送出されることになる。

【００２７】

このように送信されたデータＤＴｓを受信する受信装置２では、まず伝送路３から供給されてきたデータＤＴｓを受信部２１で受信し、復号部２２に供給する。復号部ではデータＤＴｓに対する暗号解読処理を行うことで、暗号化前のデー

タ、即ち乱数データが付加されている状態のデータＤＴａｄが出力される。

このデータＤＴａｄはブロックデコード部２３に供給され、ランダムデータ部分が除去されるとともに、データＤＴ、付加データＤａ１、Ｄａ２が抽出される。つまり当初の送信データが得られることとなる。

【００２８】

ここで破線で示すように、何らかの手段で伝送路３から暗号化されたデータＤＴｓが取り出された場合を考える。

上述したようにデータＤＴｓにおいて元の内容が明白な部分（例えば付加データＤａ２となるＩＳＲＣ）が抽出されると暗号化アルゴリズムが解読されるおそれがある。

しかしながら本例の場合、付加データＤａ２は、一連のブロックシーケンスのうちでどのブロックに挿入されるかは、全くランダムなものとなるようにしている。従って実際上、伝送路３から暗号化データＤＴｓを抽出しようとする悪意のユーザーにとって、付加データＤａ２に相当する部分としての暗号化データＤＴｓを抽出することは不可能となる。つまり「元の内容が明白なデータ」の部分の暗号化データＤＴｓは抽出できない。従って暗号解読は困難となる。

【００２９】

また、仮にデータＤＴｓにおいて、付加データＤａ２の部分が抽出されたとしても、データＤＴｓは、乱数データを含めた上で暗号化されているため、データＤＴｓの解析処理において、データＤＴｓ上では暗号化アルゴリズムによるデータ要素と乱数データによるデータ要素を区別することはできず、従って、暗号化アルゴリズムを解析することは一層困難となる。

【００３０】

以上のことから、本例によれば伝送路３で伝送されるデータについて暗号解読はほぼ不可能となり、従って、著作権保護を要するデータの伝送などに非常に好適なものとなる。

また送信装置１側では、ブロック処理部１０で付加データＤａ２の挿入ブロックをランダム化するという処理、及びランダムデータ付加部１１で乱数データを挿入するという処理を加えるだけでよく、送信装置１としての構成がさほど複雑

化することもない。従って各種の機器への導入は容易なものとなる。

【００３１】

なお付加データＤａ２の挿入ブロックをランダム化しても、受信装置２側ではデコードが困難になることはない。詳しくは後述するが、付加データＤａ２を明示するラベルがブロック内に配されていることで、受信装置２のブロックデコード部２３は、そのラベルに応じて付加データを抽出すればよいためである。また乱数データの除去も同じ理由で容易である。つまりブロック内の無効データ部分に乱数データを挿入するため、ブロックデコード部２３はラベルによって無効データ部分とされている部分を捨て去ればよいのみとなる。

従って受信装置２としての構成も複雑化することもなく、各種の機器への導入は容易である。

【００３２】

２．ＩＥＥＥ１３９４の伝送フォーマット

ここでＩＥＥＥ１３９４による伝送フォーマットについて説明する。

ＩＥＥＥ１３９４方式でのデータ伝送では、例えば図２（ａ）に示すように、所定の通信サイクル（例えば１２５μｓｅｃ）毎に時分割多重によって行われる。そして、この信号の伝送は、サイクルマスタと呼ばれる機器（ＩＥＥＥ１３９４バス上の任意の１台の機器）が通信サイクルの開始時であることを示すサイクルスタートパケットＣＳＰをバス上へ送出することにより開始される。なお、サイクルマスタは、バスを構成するケーブルに各機器を接続したとき等に、ＩＥＥＥ１３９４で規定する手順により自動的に決定される。

【００３３】

１通信サイクル中における通信の形態は、ビデオデータやオーディオデータなどのリアルタイム性を必要とするデータを伝送するアイソクロナス伝送（Ｉｓｏ）と、制御コマンドや補助的なデータなどを確実に伝送するアシンクロナス伝送（Ａｓｙ）の２種類の伝送が行われる。

各通信サイクル中では、アイソクロナス伝送用のアイソクロナスパケットＩｓｏが、アシンクロナス伝送用のアシンクロナスパケットＡｓｙより先に伝送される。

アイソクロナスパケットＩｓｏの通信が終了した後、次のサイクルスタートパケットＣＳＰまでの期間が、アシンクロナスパケットＡｓｙの伝送に使用される。従って、アシンクロナスパケットＡｓｙが伝送できる期間は、そのときのアイソクロナスパケットＩｓｏの伝送チャンネル数により変化する。また、アイソクロナスパケットＩｓｏは、１通信サイクル毎に予約した帯域（チャンネル数）が確保される伝送方式であるが、受信側からの確認は行わない。

アシンクロナスパケットＡｓｙで伝送する場合には、受信側からアクノリッジメント（Ａｃｋ）のデータを返送させて、伝送状態を確認しながら確実に伝送させる。

【００３４】

図２（ｂ）に、ＣＩＰ(Common Isochronos Packet)の構造を示す。つまり、図２（ａ）に示したアイソクロナスパケットＩｓｏのデータ構造である。

例えば、上述した１ビットデジタルオーディオデータは、ＩＥＥＥ１３９４通信においては、アイソクロナス通信によりデータの送受信が行われる。つまり、リアルタイム性が維持されるだけのデータ量をこのアイソクロナスパケットに格納して、１アイソクロナスサイクル毎に順次送信するものである。

【００３５】

アイソクロナスパケットは、図２（ｂ）のように、１３９４パケットヘッダ、ヘッダＣＲＣ、ＣＩＰヘッダ、データ部、データＣＲＣから成る。

このＣＩＰ構造として、例えば２チャンネルの１ビットデジタルオーディオデータの伝送に用いる場合における具体例を図３に示している。

【００３６】

図3では、横方向に３２ビット（４バイト）を示しているが、その１行分のデータ、つまり３２ビットが１カドレット（ｑｕａｄｌｅｔ）と呼ばれる。

ＣＩＰの先頭３２ビット（１カドレット）は、１３９４パケットヘッダとされている。

１３９４パケットヘッダにおいては、１６ビットのデータレングス（ｄａｔａ＿Ｌｅｎｇｔｈ）、２ビットのタグ（ｔａｇ）、６ビットのチャンネル（ｃｈａｎｎｅｌ）、４ビットのタイムコード（ｔ　ｃｏｄｅ）、４ビットのシンク（ｓｙ）が配される。

そして、１３９４パケットヘッダに続く１カドレットの領域はヘッダＣＲＣが格納される。

【００３７】

ヘッダＣＲＣに続く２カドレットの領域がＣＩＰヘッダとなる。

ＣＩＰヘッダの上位カドレットの先頭２バイトには、それぞれ‘０’‘０’が格納され、続く６ビットの領域はＳＩＤ（送信ノード番号）を示す。ＳＩＤに続く８ビットの領域はＤＢＳ（データブロックサイズ）であり、データブロックのサイズ（パケット化の単位データ量）が示される。続いては、ＦＮ（２ビット）、ＱＰＣ（３ビット）の領域が設定されており、ＦＮにはパケット化する際に分割した数が示され、ＱＰＣには分割するために追加したカドレット数が示される。

ＳＰ（１ビット）にはソースパケットのヘッダのフラグが示され、ＤＢＣにはパケットの欠落を検出するカウンタの値が格納される。

なお、図中「ｒｓｖ」はリザーブ、つまり未定義の領域を示している。

【００３８】

ＣＩＰヘッダの下位カドレットの先頭２バイトにはそれぞれ‘１’‘０’が格納される。そして、これに続いてＦＭＴ（６ビット）、ＦＤＦ（８ビット）、ＳＹＴ（１６ビット）の領域が設けられる。

ＦＭＴには信号フォーマット（伝送フォーマット）が示され、ここに示される値によって、当該ＣＩＰに格納されるデータ種類（データフォーマット）が識別可能となる。具体的には、ＭＰＥＧストリームデータ、Ａｕｄｉｏストリームデータ、デジタルビデオカメラ（ＤＶ）ストリームデータ等の識別が可能になる。

ＦＤＦは、フォーマット依存フィールドであり、上記ＦＭＴにより分類されたデータフォーマットについて更に細分化した分類を示す領域とされる。オーディオに関するデータであれば、例えばリニアオーディオデータであるのか、ＭＩＤ

Ｉデータであるのかといった識別が可能になる。

例えば１ビットデジタルオーディオデータであれば、先ずＦＭＴによりＡｕｄｉｏストリームデータの範疇にあるデータであることが示され、ＦＤＦに規定に従った特定の値が格納されることで、そのＡｕｄｉｏストリームデータは１ビットデジタルオーディオデータであることが示される。

ＳＹＴは、フレーム同期用のタイムスタンプが示される。

【００３９】

このようなＣＩＰヘッダに続けては、ＦＭＴ，ＦＤＦによって示されるデータが、データ部としてのｎ個のデータブロック（ブロック＃０～＃ｎ）のシーケンスによって格納される。ＦＭＴ，ＦＤＦにより１ビットデジタルオーディオデータであることが示される場合には、このデータブロックとしての領域に１ビットデジタルオーディオデータが格納される。

そして、データブロックに続いて最後にデータＣＲＣが配置される。

【００４０】

この図３では、データ部に２チャンネルの１ビットデジタルオーディオデータが配されている例を示している。これは、ＩＥＥＥ１３９４バスによるデータ伝送について適用できるＡＭ８２４と呼ばれる伝送プロトコルに基づいた例であり、その場合において１ビットデジタルオーディオデータとして２チャンネルのオーディオデータを伝送する場合のパケット構造例である。

【００４１】

上述のように３２ビット（４バイト）を１カドレット（Quadlet）と呼ぶとすると、２チャンネルデータの場合、４カドレット（ｑ１～ｑ４）で１つのブロックが形成され、このブロックが連続するものとなる。

【００４２】

各カドレットにおける先頭のバイト（バイト０）は、ラベルとされている。ラベルとは、そのカドレットに配されるデータの識別情報となる。

ラベルとしての値及び意味を図４に示す。

図示するようにラベル値に対して各種の意味が定義されており、例えばラベル値４０ｈ～４Ｆｈは、ＤＶＤ（Digital Versatile Disc）システムで採用されて

いるマルチビットリニアオーディオデータに対応するものとされる。なお、「ｈ」を付した数値は１６進表記のものである。

またラベル値５０ｈ～５７ｈは、１ビットデジタルオーディオデータに対応する値、ラベル値５８ｈ～５Ｆｈは、エンコードされた１ビットデジタルオーディオデータに対応する値、ラベル値８０ｈ～８３ｈはＭＩＤＩデータに対応する値とされる。

さらにＣ０ｈ～ＥＦｈはアンシラリデータ（Ancillary Data；補助データ）を意味するなど、ラベル値は識別情報として機能するために各種定義されている。

【００４３】

各ラベル値についての詳細な定義の説明は本発明と直接関係がないため説明を省略するが、図３に示した値についてのみ述べると次のようになる。

【００４４】

図３においてブロック＃０の第１カドレットｑ１をみると、ラベル値は「Ｄ１ｈ」とされている。従って第１カドレットｑ１はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト１はサブラベルとされて「００ｈ」とされている。

このときバイト２，バイト３が実際の補助データ内容となるが、ここではバリディティフラグ（Validity Flag）Ｖ、コピーコントロール情報（Track Attribute）、チャネル数（Ch Bit Num）、スピーカ配置情報（Loudspeaker Config）が記述される。

【００４５】

第２カドレットｑ２ではラベル値は「５０ｈ」とされる。ラベル値５０ｈ～５７ｈは、１ビットデジタルオーディオデータに対応する値であるが、「５０ｈ」は、マルチチャンネルのデータを配したブロックの最初のデータであることを示す。

また第３カドレットｑ３ではラベル値は「５１ｈ」とされる。「５１ｈ」は、マルチチャンネルのデータを配したブロックの２番目以降のデータであることを示す。

従って、第２、第３カドレット（ｑ２、ｑ３）では、チャンネル１（例えばＬ

チャンネル）、チャンネル２（例えばＲチャンネル）の２チャンネルの１ビットデジタルオーディオデータが配されていることが示されるものとなる。各チャンネルのデータはバイト１～バイト３の３バイトで記述される。

【００４６】

第４カドレットｑ４では、ラベル値は「ＣＦｈ」とされている。これはアンシラリデータの範疇であるが、「ＣＦｈ」は特に無効データ（NO DATA）を示す値として定義されている。またバイト１はサブラベルとして無効データの内容を示す値とされており、この例では「ＣＦｈ」とされている。

そしてこのときバイト２，バイト３が無効データにより充填される。

なお、第４カドレットｑ４として無効データが配されるカドレットが形成されるのは、１つのブロックは偶数個のカドレットで形成されるべく規定されているためである。

【００４７】

ブロック＃１の第１カドレットｑ１では、ラベル値は「Ｄ１ｈ」とされている。従って第１カドレットｑ１はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト１はサブラベルとされて「０１ｈ」とされている。

このときはバイト２，バイト３の補助データ内容は、サプリメンタリデータとされる。

第２～第４カドレットはブロック＃０と同様である。

【００４８】

このように各ブロックが構成されて、アイソクロナスパケットＩｓｏにおけるデータ部が形成される。

なお、ここで示したアンシラリデータ、サプリメンタリデータは、図１に示した付加データＤａ１に相当するデータとなる。従ってこれらは、例えば１ビットデジタルオーディオデータとともにメディア上に記録されていた付加データであって、その段階で既に暗号化された内容のデータであるとする。

付加データＤａ２となる例えばＩＳＲＣについては図３では示していないが、続いて図５以降で説明するように、例えばラベルが「Ｃ０ｈ」、サブラベルが「

０１ｈ」以降の値として設定されたカドレットに配されることとなる。なお、このラベルの値は一例にすぎない。

【００４９】

３．ＩＥＥＥ１３９４でオーディオパケットデータを伝送する場合の付加データのランダム挿入例

以上のようなＩＥＥＥ１３９４による伝送フォーマットを用いて、図１で説明したようにデータを伝送する場合の具体例を以下、説明していく。即ちＩＥＥＥ１３９４の伝送路３でオーディオパケットデータを伝送する場合のブロックシーケンスの例である。

【００５０】

まず図５でブロックシーケンスの概要を述べる。

上記図３で示したデータ部を構成するブロック＃０、＃１・・・に配されるオーディオデータは、元々の１ビットデジタルオーディオデータとしてのトラック（楽曲単位）から見ると図５に示す関係となる。

図５（ａ）は１つの楽曲としてのデータ群となるトラック（プログラム）をトラック＃Ｎとして示しているが、このトラック＃Ｎは図５（ｂ）のように複数のフレームから構成される。

公知のように１つのフレームは７５Ｈｚ周期、即ち１３．３ｍｓｅｃ分のオーディオデータに相当する単位である。

そして図５（ｃ）のように１フレームは１５６８ブロック（ブロック＃０～＃１５６７）で構成される。

なお、図５にフレームとして示すブロック＃０～＃１５６７の部分は、図２，図３で説明したアイソクロナスパケットＩｓｏ内のデータ部に相当する部分である。

【００５１】

図５（ｄ）は、ブロック＃０～＃１５６７の内容の例を示したものである。２

チャンネルの１ビットデジタルオーディオデータの伝送を考えた場合、上記図３で説明したように各ブロックは４カドレット（ｑ１～ｑ４）で形成され、カドレットｑ２，ｑ３にオーディオデータが配される。

そして上述のようにカドレットｑ４はラベルが「ＣＦｈ」とされて、無効データが配される部分となる。

【００５２】

また図３で説明したように第１カドレットｑ１はアンシラリデータＡｎｃｉ、サプリメンタリデータＳｕｐｐｌｉが配されるが、フレームを構成する先頭のブロック＃０は、ラベル、サブラベルが「Ｄ１ｈ」「００ｈ」とされて、図３に示したようにアンシラリデータＡｎｃｉ（付加データＤａ１）が配される。

またブロック＃１以降は、カドレットｑ１は、ラベル、サブラベルが「Ｄ１ｈ」「０１ｈ」とされて、サプリメンタリデータＳｕｐｐｌｉ（付加データＤａ１）が配される。

なお、先頭ブロック＃０にアンシラリデータＡｎｃｉが配されることはＡＭ８２４の伝送フォーマット上、規定されているが、ブロック＃１～＃１５６７においては、カドレットｑ１にどのようなデータを配しなければならないかは規定されていない。ただし通常はブロック＃１から所定数のブロックに連続して、サプリメンタリデータＳｕｐｐｌｉが配されることになる。

【００５３】

また或るブロック＃ｙのカドレットｑ１は、ラベルが「Ｃ０ｈ」とされて、ＩＳＲＣ等の付加データＤａ２が配される。

また、これら付加データＤａ１、Ｄａ２を配する必要がなくなったブロックとして、この場合ブロック＃ｚ、＃１５６７を例に挙げているが、それらのブロックはラベル、サブラベルが「ＣＦｈ」「Ｄ１ｈ」とされて、無効データが配される。

【００５４】

このようなブロック＃０～＃１５６７が、伝送するデータの１フレームに相当する、一連の連続したブロックシーケンスとなるが、まずこの図５（ｄ）を用いて、本例のブロック処理部１０で設定されるブロックシーケンスの説明の前に、

ランダムデータ付加部１１での乱数データの挿入方式を説明する。

【００５５】

図５（ｄ）のようなブロックシーケンスに対して、送信装置１のランダムデータ付加部１１では、無効データの部分に乱数データを挿入すればよい。即ち各ブロックにおいて斜線部を付した無効データ部分に乱数データを挿入する。

具体的にはランダムデータ付加部１１では１パケットあたりに２バイトの乱数データを生成し、無効データのカドレット、つまりラベル値＝「ＣＦｈ」のカドレットのバイト２，３の２バイトに挿入するものである。

【００５６】

このように乱数データを挿入することにより、パケット内のオーディオデータが仮にオールゼロ、あるいは「９６ｈ」などの固定パターンであったり、ＩＳＲＣ等の付加データＤａ２として、暗号化部１２での暗号化前の元のデータ内容が明白な部分があったとしても、そのデータと乱数データが混在した状態で暗号化されることになるため、元のデータ内容が見えないものとなる。つまり上述のように暗号解読を困難にできる。

なお、暗号化部１２で暗号化処理を行うデータ単位がブロック単位より小さい単位、例えば８バイト（２カドレット）単位であった場合は、その８バイト毎に、一部に乱数データが挿入されるようにすることが好ましい。

【００５７】

本例の送信装置のブロック処理部１０では、一連のブロック＃０～＃１５６７の中で、付加データＤａ２を挿入するブロックをランダムに選択するものである。

この処理を図６，図７で説明する。

図６、図７は、図５（ｄ）に示した１フレーム内のブロックシーケンスを、各ブロックの第１カドレットｑ１のみで示している。

【００５８】

なお、図６（ａ）として、比較のために通常のブロックシーケンスを示す。

図６（ａ）の通常のブロックシーケンスの場合は、先頭ブロック＃０にアンシラリデータＡｎｃｉが配され、続いてブロック＃１～＃（ｘ－１）まで連続して

サプリメンタリデータＳｕｐｐｌｉが配される。つまり先頭ブロックから順に付加データＤａ１が配されていく。

もしＩＳＲＣ等の付加データＤａ２を挿入することが不要な場合は、ブロック＃（ｘ）～＃１５６７については、カドレットｑ１は無効データ部分とされるが、付加データＤａ２を挿入する場合は、サプリメンタリデータＳｕｐｐｌｉに続いて、ブロック＃（ｘ）以降に順に付加データＤａ２（ＩＳＲＣ等）が挿入される。図６（ａ）の例の場合は、ブロック＃（ｘ）～ブロック＃（ｘ＋２）は、それぞれラベルが「Ｃ０ｈ」で、サブラベルが順に「００ｈ」「０１ｈ」「０２ｈ」とされて、それぞれＩＳＲＣとしての情報が挿入されている。

そしてブロック＃（ｘ＋３）～ブロック＃１５６７までは無効データ（斜線部）が充填される。なお、上述のようにこの無効データ部分には乱数データが挿入されることになる。

【００５９】

しかしながらこのような通常のブロックシーケンスによれば、ＩＳＲＣが挿入された位置（ブロックのナンバ）が悪意のユーザーにとって予測し得るものとなるおそれがある。つまり付加データＤａ１の挿入に用いられるブロック数が固定的であるとすると、その次のブロック＃ｘがＩＳＲＣが挿入されたブロックであるとわかってしまう。すると、暗号化データＤＴｓのうちでブロック＃ｘの部分を抽出するとともに、何らかの手段で伝送されている楽曲についてのＩＳＲＣを知ると、暗号化アルゴリズムが解析しやすくなってしまう。

【００６０】

そこで本例のブロック処理部１０では上述のように、少なくとも付加データＤａ２については、ランダムにブロックを選択して挿入するようにする。

図６（ｂ）が付加データＤａ２をランダムに挿入する場合のブロックシーケンスの例である。

図示するように先頭のブロック＃０にアンシラリデータＡｎｃｉが配され、続いてブロック＃１～＃（ｘ－１）まで連続してサプリメンタリデータＳｕｐｐｌｉが配されることは通常のブロックシーケンスと同様としている。

【００６１】

ここで付加データＤａ２はブロック＃（ｘ）以降に挿入されるものとなるが、付加データＤａ２を挿入するブロックは、ブロック＃（ｘ）～＃１５６７のうちでランダムに選択するようにする。

例えばこの図６（ｂ）の場合は、付加データＤａ２としてのＩＳＲＣが、ブロック＃（ｘ＋１）、＃（ｘ＋２）、＃１５６７に挿入されている。

そしてこれら以外のブロックは無効データ（斜線部）が配される。これはランダムデータ付加部１１で乱数データが配される領域となる。

【００６２】

このようにブロック＃（ｘ）～＃１５６７において付加データＤａ２がランダムに挿入されることは、各フレーム毎に行われる。

例えば図６（ｂ）がフレーム＃Ｍのブロックシーケンスであるとすると、次のフレーム＃（Ｍ＋１）は、図７のようになる。例えばこの場合は、付加データＤａ２としてのＩＳＲＣが、ブロック＃（ｘ）、＃（ｘ＋３）、＃１５６６に挿入されている。そしてこれら以外のブロックは無効データ（斜線部）が配される。

【００６３】

即ち本例では、ブロック処理部１０において、各フレームを構成するブロックシーケンス内で、付加データＤａ２についてはブロック＃ｘ～＃１５６７内のランダムに選択したブロックに挿入するようにしている。

従って、各フレームを構成するデータストリーム内では、どのブロックに付加データＤａ２が挿入されているかは、全く予測できないものとなる。

そしてこのようなブロックシーケンスのデータが暗号化部１２で暗号化データＤＴｓとされて伝送路３に送出されるが、伝送路３から暗号化データＤＴｓのうちで付加データＤａ２部分を抽出することはほぼ不可能となる。このため上述のように不正な暗号アルゴリズムの解析を防止できる。

また、上記のように無効データ部分に乱数データが挿入されることで、一層暗号アルゴリズムの解析を困難とすることができる。

【００６４】

なお、以上のように付加データＤａ２がランダムなブロックに挿入されること

や、それによってフレーム毎に付加データＤａ２の位置が異なることとなっても受信装置２側では不都合はない。

つまり受信装置２のブロックデコード部２３では、単に各フレームを構成するブロックから、ラベル＝「Ｃ０ｈ」の部分を抽出すればよいためである。

【００６５】

また、無効データ部分に乱数データを挿入することによっても、受信装置２側での処理が複雑とはならない。

即ち受信装置２のブロックデコード部２３はラベル値＝「ＣＦｈ」のカドレットを捨てればよいのみであるためである。ラベル値＝「ＣＦｈ」のカドレットは無効データとして本来捨てられるものであるため、その意味でいえば、乱数データ除去のために何ら特別な処理を必要としないものともなる。

【００６６】

ところで、ブロック処理部１０でのブロックシーケンスの設定は、図８の例に示すように行ってもよい。

上記図６（ｂ）及び図７の例は、ブロック＃（ｘ）以降で付加データＤａ２を挿入する位置をランダムに選択したが、図８の例はブロック＃１～＃１５６７までをランダムに選択する対象とする例である。

【００６７】

つまり、先頭のブロック＃０についてはラベル、サブラベルが「Ｄ１ｈ」「００ｈ」のアンシラリデータＡｎｃｉを挿入するものと規定されているため、これを変えることはできないが、ブロック＃１以降は任意である。そしてラベル、サブラベルでデータ内容が規定される限り、付加データＤａ１としてのサプリメンタリデータＳｕｐｐｌｉや、付加データＤａ２としてのＩＳＲＣは、どのブロックに挿入されていても、受信装置側では問題ない。

そこで、図８のようにサプリメンタリデータＳｕｐｐｌｉを含めて、挿入するブロックをランダムに選択するようにしてもよい。

【００６８】

図８の例の場合は、或るフレームにおいて付加データＤａ１としてのサプリメンタリデータＳｕｐｐｌｉが、ブロック＃３、＃４、＃（ｘ＋２）、＃１５６７

・・・に配されており、また付加データＤａ２としてのＩＳＲＣが、ブロック＃２、＃４、＃（ｘ）・・・に配されている。

これらの付加データが挿入されなかったブロックは無効データが充填される（斜線部）。

もちろんこの図８は、或るフレームにおいてサプリメンタリデータＳｕｐｐｌｉ及びＩＳＲＣがランダムなブロックに挿入された場合の一例であり、次のフレーム、その次のフレームなどでは、サプリメンタリデータＳｕｐｐｌｉやＩＳＲＣの順序は全く別の状態となる。

【００６９】

このようにサプリメンタリデータＳｕｐｐｌｉまでをも含めて、付加データＤａ１，Ｄａ２の挿入ブロックをランダムに選択することにより、例えばＩＳＲＣなどの元の内容が明白なデータが挿入されている位置は、一段と予測できないものとなり、暗号解読の防止効果を強めることができる。

きな

【００７０】

４．記録装置に本発明を採用する例

続いて、本発明のデータ送出装置（データ送出方法）を、所定のメディアにデータを記録する記録装置に採用する実施の形態を説明する。

【００７１】

図９は所定の記録媒体（メディア）６に対してデータＤＴ（及び付加データＤａ１，Ｄａ２）を記録できる記録装置である。

図示するように記録装置４は、入力されてくるデータＤＴに対する記録処理系として、暗号化部４０，エンコード及び記録ドライブ部４４、記録ヘッド（又はインターフェース）４５が設けられる。

暗号化部４０は、ブロック処理部４６，ランダムデータ付加部４１，暗号化部４２、送出部４３を有する。

【００７２】

このような記録装置４に対しては、上記の送信装置１の場合と同様に、例えば光ディスク、ハードディスク、メモリカード等の所要のメディア６に対して記録するデータとして、例えば１ビットデジタルオーディオデータなどのデータＤＴ、及びこの主たるデータＤＴに付随する付加データＤａ１が供給され、また例えばＩＳＲＣなどの付加データＤａ２が供給されるものとする。

【００７３】

ブロック処理部４６は、データＤＴ、付加データＤａ１，Ｄａ２について、上述したＩＥＥＥ１３９４による伝送フォーマットに即したブロックとしてのデータストリームに形成する処理を行う。

そして少なくとも付加データＤａ２については、或いは付加データＤａ１，Ｄａ２について、連続するブロックのうちでランダムに選択したブロック内に配置されるようにする。即ち図６，図７或いは図８で説明したようにブロックシーケンスを設定する。

【００７４】

またランダムデータ付加部４１は内部に乱数発生回路から発生させた乱数データを、ブロックの所要の部分、例えば無効データ部分に付加する。

ランダムデータ付加部４１で乱数データが挿入されたデータＤＴａｄは、続いて暗号化部４２に供給され、暗号化処理が施される。

暗号化されたデータＤＴｓは、送出部４３に供給され、送出部４３からエンコード及び記録ドライブ部４４に送出される。

【００７５】

エンコード及び記録ドライブ部４４は、供給されたデータＤＴｓに対して、記録を行うメディア６の記録フォーマット、変調方式に応じてエラー訂正符号の付加や各種エンコード処理を行い、記録ドライブ信号を生成する。

その記録ドライブ信号は記録ヘッド４５に供給されて記録ヘッド４５によりメディア６へのデータ書込が行われる。

例えばメディア６が光ディスク、光磁気ディスク、磁気ディスク、磁気テープなどであれば、記録ドライブ信号に応じて光学ヘッド又は磁気ヘッドが駆動され

て記録が実行される。

また、メディア６がフラッシュメモリなどによるメモリカードのような形態であれば、インターフェース４５によりメディア６に対して書込アクセスが行われることになる。

【００７６】

図１０は所定の記録媒体（メディア）６からデータＤＴを再生できる再生装置である。

図示するように再生装置５は、メディア６からデータの読み出しを行う再生ヘッド（又はインターフェース）５４、デコード部５５、復号部５０が設けられる。

復号部５０は、取込部５１，復号部５２、ブロックデコード部５３を備える。

【００７７】

この再生装置５では、例えばメディア６としての光ディスク、光磁気ディスク、磁気ディスク、磁気テープなどから光学ヘッド又は磁気ヘッドとしての再生ヘッド５４によって読み出されたデータ、或いはメディア６としてのメモリカードからインターフェース５４を介した読出アクセスにより読み出されたデータは、デコード部５５で、メディア６の記録フォーマットに応じたデコード処理やエラー訂正処理が行われる。そしてそのデコードされたデータは、即ち記録装置４で暗号化されたデータＤＴｓであり、データＤＴｓは取込部５１により復号部５０内に取り込まれ、復号部５２で暗号解読処理される。

復号部５２で、上記暗号化部４２での暗号化アルゴリズムに対応した暗号解読処理を行うことで、ランダムデータが付加された状態のデータＤＴａｄとされる。そして、そのデータＤＴａｄがブロックデコード部５３でランダムデータの除去処理が行われるとともに、付加データＤａ１，Ｄａ２の抽出、データＤＴの抽出が行われて、元のデータＤＴや付加データＤａ１，Ｄａ２が再生されるものとなる。

【００７８】

記録装置４が以上のように構成されることで、メディア６に記録されるデータにおいて、ＩＳＲＣ等の付加データＤａ２として元の内容が明白なデータは、ブ

ロックシーケンス上では位置が全く予測できないものとなる。

従ってメディア６に記録されたデータをデコードしても、付加データＤａ２に相当するデータ部分を抽出することは困難となり、この点で暗号解読は困難となる。

さらに乱数データが付加された後に暗号化されることで、暗号化前の段階で元のデータ内容が明白な部分がなくなる。

従ってメディア６から仮にＩＳＲＣ等の付加データＤａ２に相当する部分が抽出されても、そのデータは、乱数データを含めた上で暗号化されているため、データＤＴｓの解析処理において、データＤＴｓ上では暗号化アルゴリズムによるデータ要素と乱数データによるデータ要素を区別することはできず、従って、暗号化アルゴリズムを解析することはほぼ不可能である。

【００７９】

つまりこのような記録装置によれば、メディア６に記録されるデータについて暗号解読は非常に困難なものとなり、従って、著作権保護を要するデータの記録などに非常に好適なものとなる。

また、上述した送信装置１の場合と同様に、記録装置４として構成がさほど複雑化することもなく、導入は容易である。

また、上述した受信装置２の場合と同様に、ランダムに挿入された付加データＤａ２の抽出や乱数データの除去は、ラベルに応じて実行すればよいため、再生装置５のブロックデコード部５３の処理は簡易なものとなる。

【００８０】

なお、図９，図１０として記録装置４、再生装置５を分けて示したが、これらの回路構成を１つの機器に設けて、記録再生装置とすることはもちろん可能である。

また、記録装置４（又は記録再生装置）としては、必ずしも暗号化部４０を設けなくてもよい。例えば伝送路３を介して或る送信装置から伝送されてきたデータを記録する記録装置を考えると、その送信装置側が図１に示した構成を備えていれば、記録装置に伝送されてくるデータは、既にランダムな位置に付加データＤａ２が配されるとともに、乱数データが付加された上で暗号化されたデータＤ

Ｔｓとなっている。従ってその場合、記録装置は暗号化部４０は不要となる。そして再生装置は、図１０に示した復号部５０を備えることで、伝送され記録されたデータの再生を行うことができるようになる。

例えば音楽等の配信システムなどを想定すると、このような形態が好適なものとなる。

【００８１】

以上、実施の形態を説明してきたが、本発明はさらに多様な構成例が考えられ、また送信装置、記録装置などの形態で多種多様な機器に導入できるものである。

また、上記例では送信装置１と受信装置２は有線としてのＩＥＥＥ１３９４方式の伝送路３による伝送システムとしたが、他の伝送規格によるものでもよく、また衛星通信、無線電話通信、赤外線伝送などの無線伝送システムに本発明を適用できることはもちろんである。

また、伝送するデータは図５～図８に示したようなブロックデータに限定されるものではなく、あらゆるデータの伝送に本発明を適用できる。

また上記例では、ブロックの無効データ部分に乱数データを挿入するようにしたが、このような処理を行わなくてもよい。例えば図１，図９のランダムデータ付加部１１，４１は設けなくてもよい。即ちブロック処理部１０，４６で付加データを挿入するブロックをランダムに選択する処理のみでも、十分に暗号解読を困難にする効果があるためである。

【００８２】

また、付加データＤａ２に相当する付加データはＩＳＲＣに限られず、予め暗号化されておらず、かつそのデータ内容がわかり得るものがあり、例えばディスクタイトル、アーティスト名、ディスク製造ナンバ等が、暗号化されないテキストデータなどでそのまま付加データとされる場合は、それらも上述の付加データＤａ２に相当する。つまり、ランダムな位置に挿入されるべき付加データとなる。

【００８３】

【発明の効果】

以上の説明からわかるように、本発明によれば、伝送するデータとしての連続したデータブロックに対して、付加データをランダムに選択したデータブロックに付加することで、付加データが付加される位置が連続するデータブロック内でランダムなものとなるようにしている。これによって、伝送されている暗号化データにおいて、「元の内容が明白なデータ」が配されている位置がわからないようにし、「元の内容が明白なデータ」に相当する暗号化データを抽出できないようにしている。これによって暗号アルゴリズムの解読を困難にできるという効果がある。

従って本発明は著作権保護などを必要とするデータの伝送に非常に好適なものとなる。

【００８４】

またデータブロックの一部に乱数データを挿入することで、より暗号アルゴリズムの解読を困難とできる。

【００８５】

またデータ送出装置は、異なる機器としての受信装置に対してデータを伝送する送信装置とすることで、機器間のデータ伝送において上記効果を実現できる。

さらにデータ送出装置は、それぞれ記録媒体に記録を行う記録装置における記録データの送出装置とすることで、記録媒体に記録されているデータ、又は記録再生の過程のデータにおいて上記効果を実現できる。

【図面の簡単な説明】

【図１】

本発明の実施の形態の送信装置及び受信装置のブロック図である。

【図２】

ＩＥＥＥ１３９４による伝送フォーマットの説明図である。

【図３】

ＩＥＥＥ１３９４のアイソクロナスパケットの説明図である。

【図４】

実施の形態のパケットデータのラベルの説明図である。

【図５】

実施の形態のブロックシーケンスの説明図である。

【図６】

実施の形態の付加データのランダムな挿入例の説明図である。

【図７】

実施の形態の付加データのランダムな挿入例の説明図である。

【図８】

実施の形態の付加データについての他のランダムな挿入例の説明図である。

【図９】

実施の形態の記録装置のブロック図である。

【図１０】

実施の形態の再生装置のブロック図である。

【図１１】

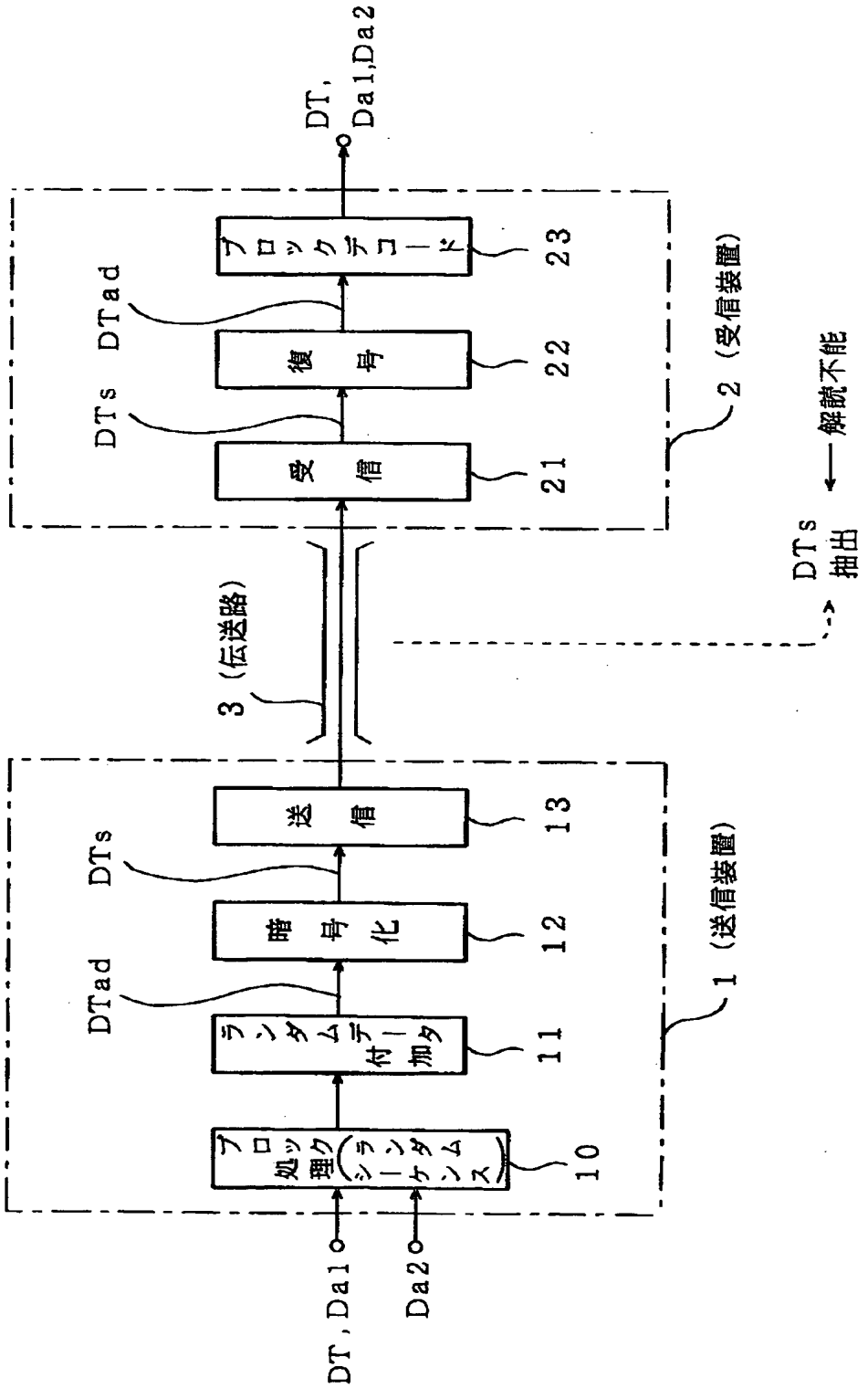
従来の伝送システムの説明図である。

【符号の説明】

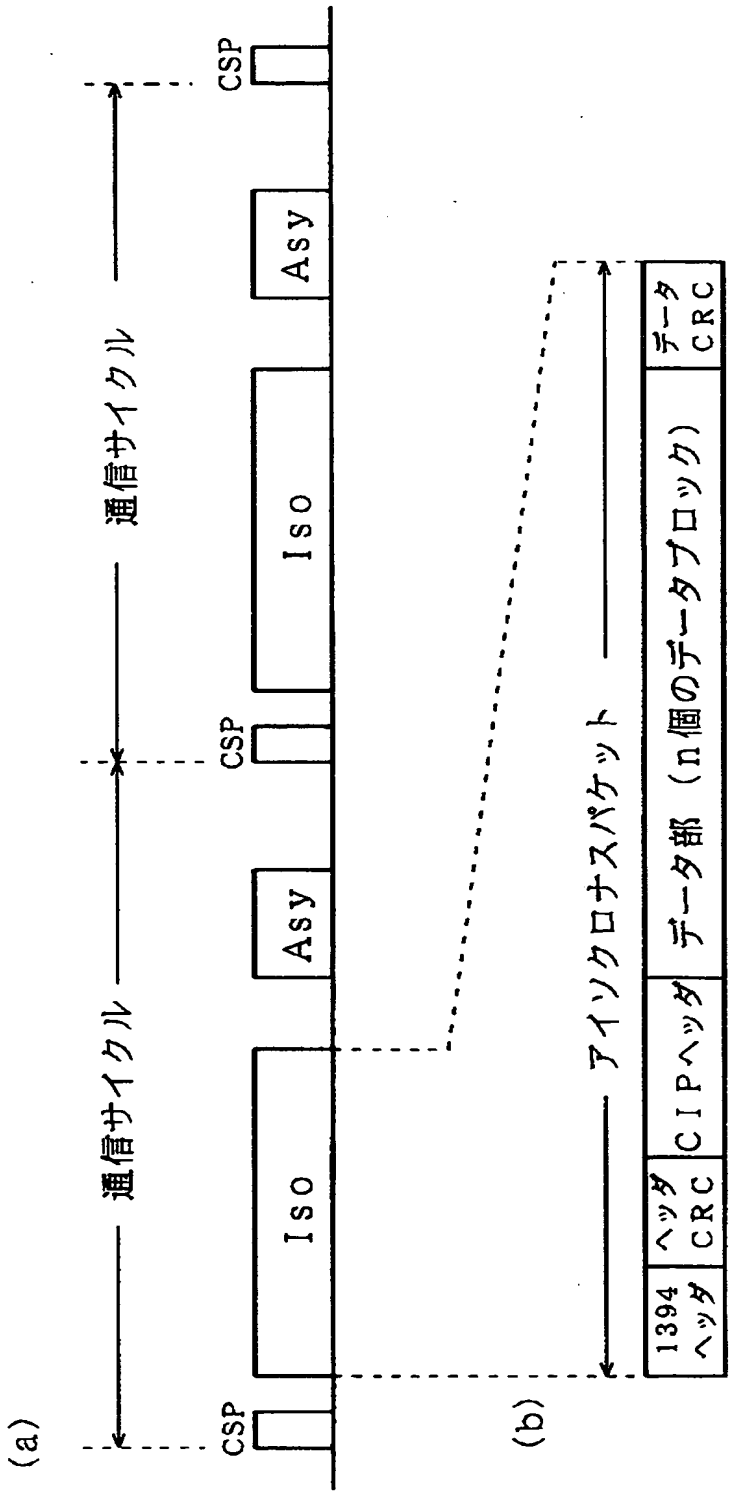
１　送信装置、２　受信装置、３　伝送路、４　記録装置、５　再生装置、６　メディア、１０，４６　ブロック処理部、１１，４１　ランダムデータ付加部、１２，４２　暗号化部、１３　送信部、２１　受信部、２２，５２　復号部、２３，５３　ブロックデコード部、４３　送出部、５１　取込部

【書類名】　　図面

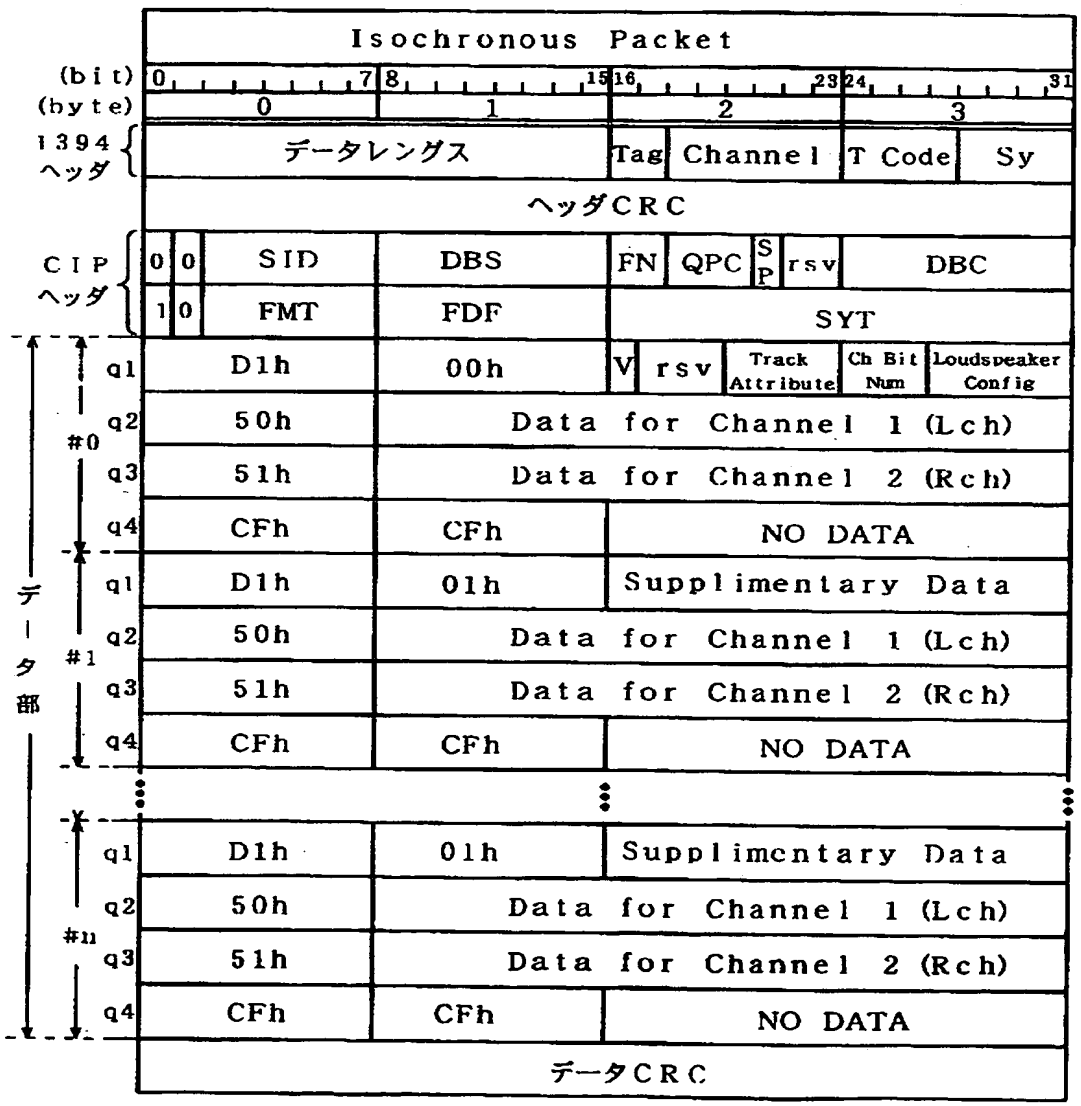
【図１】


DT,
Da1,Da2
ブロックデコード
23
復号
22
受信
21
2（受信装置）
DTs DTad
DTs
解読不能
DTs
抽出
3（伝送路）
送信
13
暗号化
12
ランダムデータ付加
11
ブロック処理（シランダムシーケンス）
10
1（送信装置）
DTad
DTs
DT,Da1
Da2

【図２】


(a)
CSP
通信サイクル
Asy
Iso
CSP
通信サイクル
Asy
Iso
CSP
(b)
アイソクロナスパケット
1394ヘッダ
ヘッダCRC
CIPヘッダ
データ部（n個のデータブロック）
データCRC

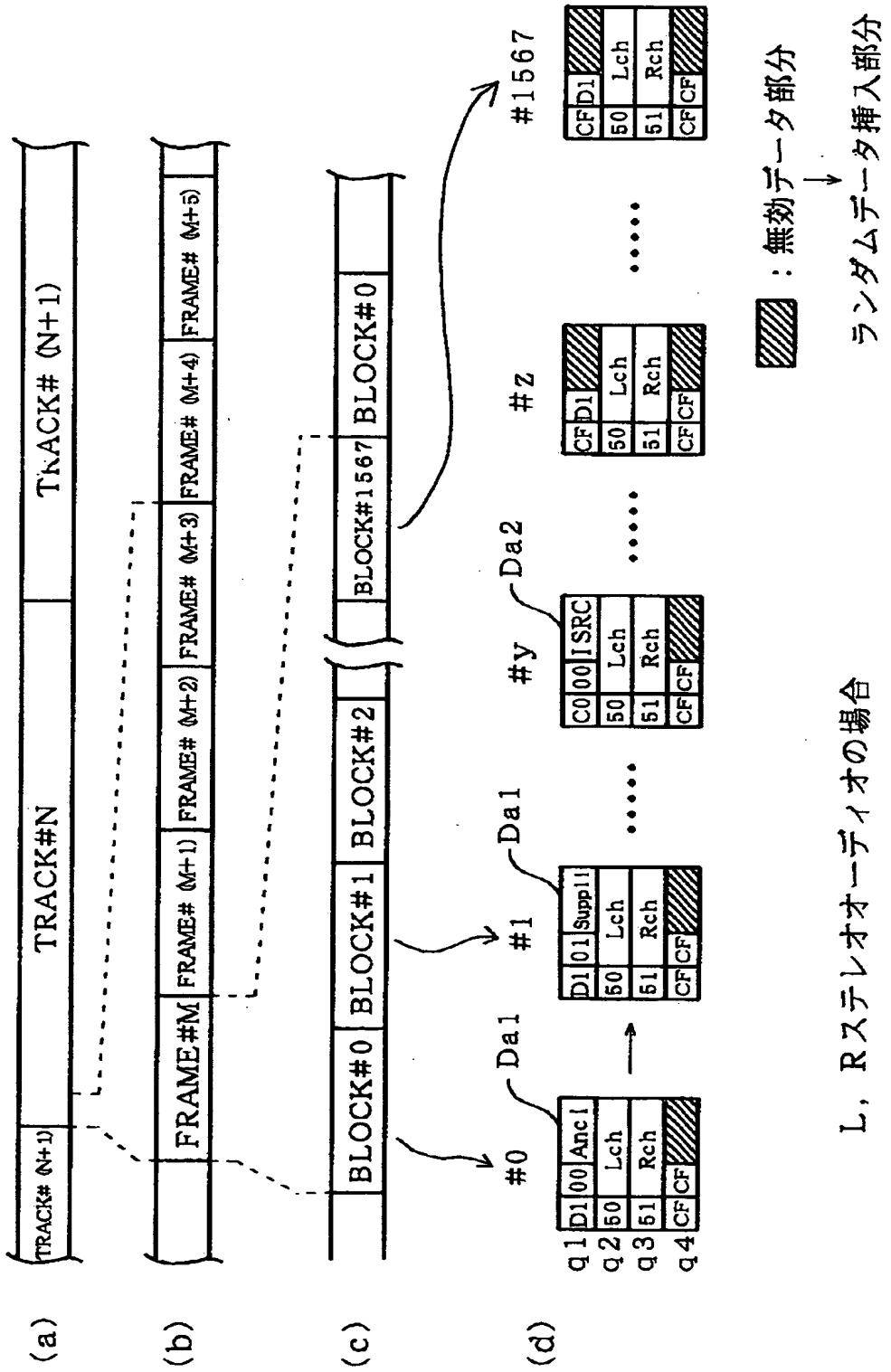
【図３】


Isochronous Packet
(bit)
(byte)
1394 ヘッダ
データレングス
Tag
Channel
T Code
Sy
ヘッダCRC
CIP ヘッダ
SID
DBS
FN
QPC
SP
rsv
DBC
FMT
FDF
SYT
データ部
#0
#1
#n
q1
q2
q3
q4
D1h
00h
V
Track Attribute
Ch Bit Num
Loudspeaker Config
50h
Data for Channel 1 (Lch)
51h
Data for Channel 2 (Rch)
CFh
NO DATA
01h
Supplimentary Data
データCRC

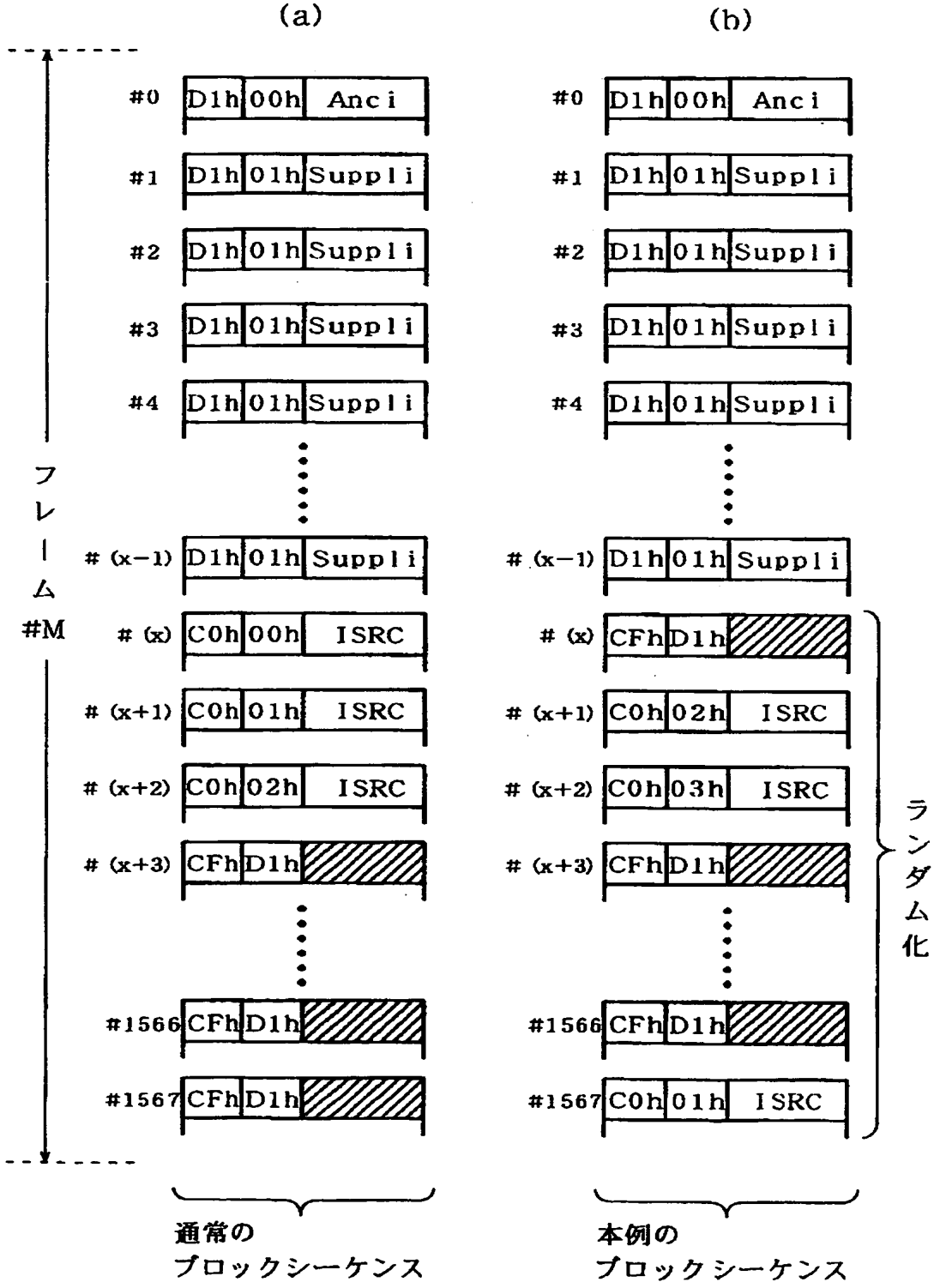
【図４】

Value	Description
00h-3Fh	IEC60958 Conformant
40h-4Fh	Multi-bit Linear Audio
50h-57h	One Bit Audio (Plain)
58h-5Fh	One Bit Audio (Encoded)
60h-7Fh	-reserved-
80h-83h	MIDI Conformant
84h-87h	Extended Music Data
88h-8Bh	SMPTE Time Code Conformant
8Ch-8Fh	Sample Count
90h-BFh	-reserved-
C0h-EFh	Ancillary Data
F0h-FFh	-reserved-

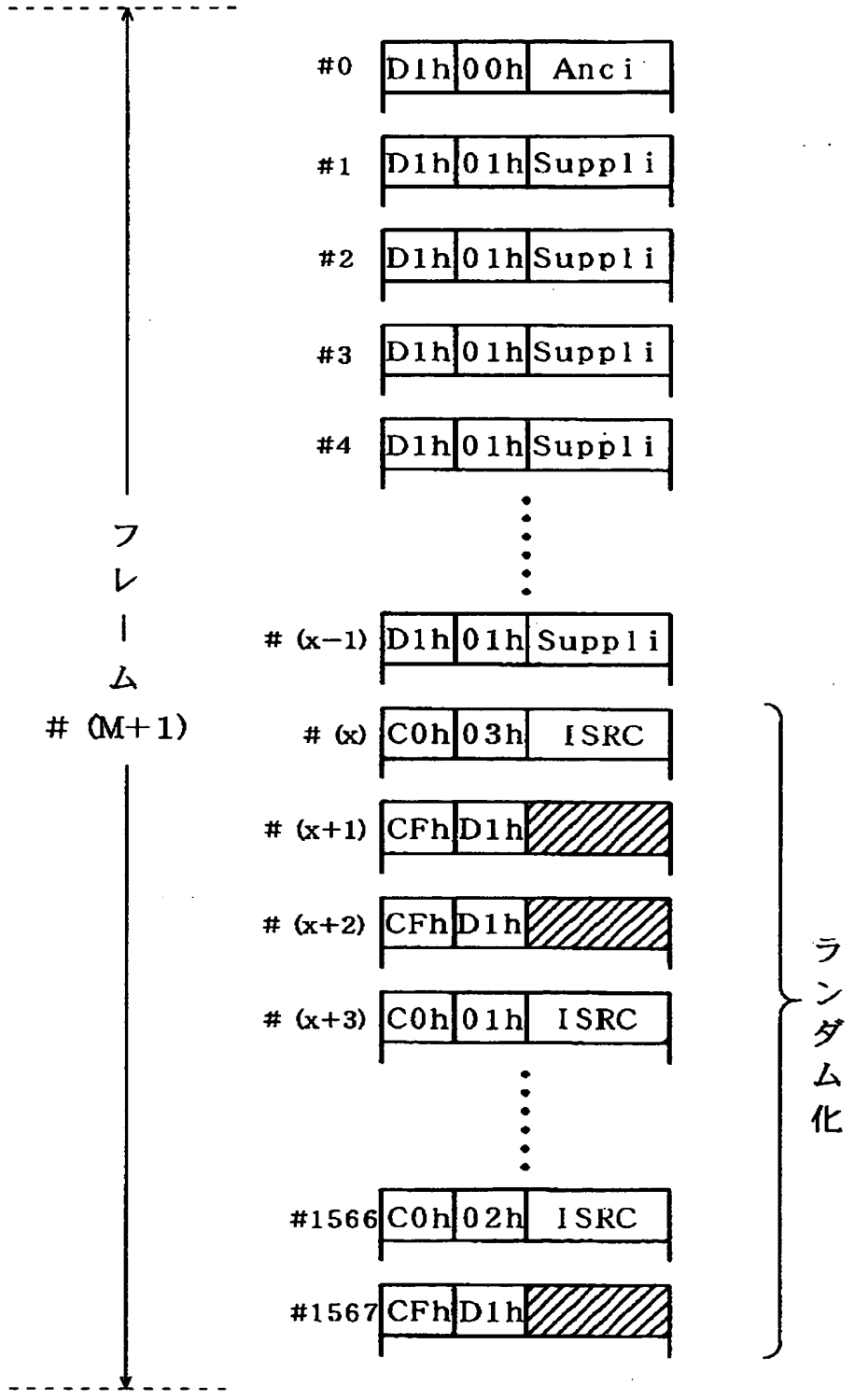
【図５】


(a)
TRACK#N
TRACK# (N+1)
TRACK# (N+1)
(b)
FRAME#M
FRAME# (M+1)
FRAME# (M+2)
FRAME# (M+3)
FRAME# (M+4)
FRAME# (M+5)
(c)
BLOCK#0
BLOCK#1
BLOCK#2
BLOCK#1567
BLOCK#0
(d)
#0
#1
#y
#z
#1567
Da1
Da1
Da2
D1 00 Ancl Lch 50 Rch 51 CF CF
D1 01 Suppl Lch 50 Rch 51 CF CF
C0 00 ISRC Lch 50 Rch 51 CF CF
CF D1 Lch 50 Rch 51 CF CF
CF D1 Lch 50 Rch 51 CF CF
q1
q2
q3
q4
：無効データ部分
ランダムデータ挿入部分
L，Rステレオオーディオの場合

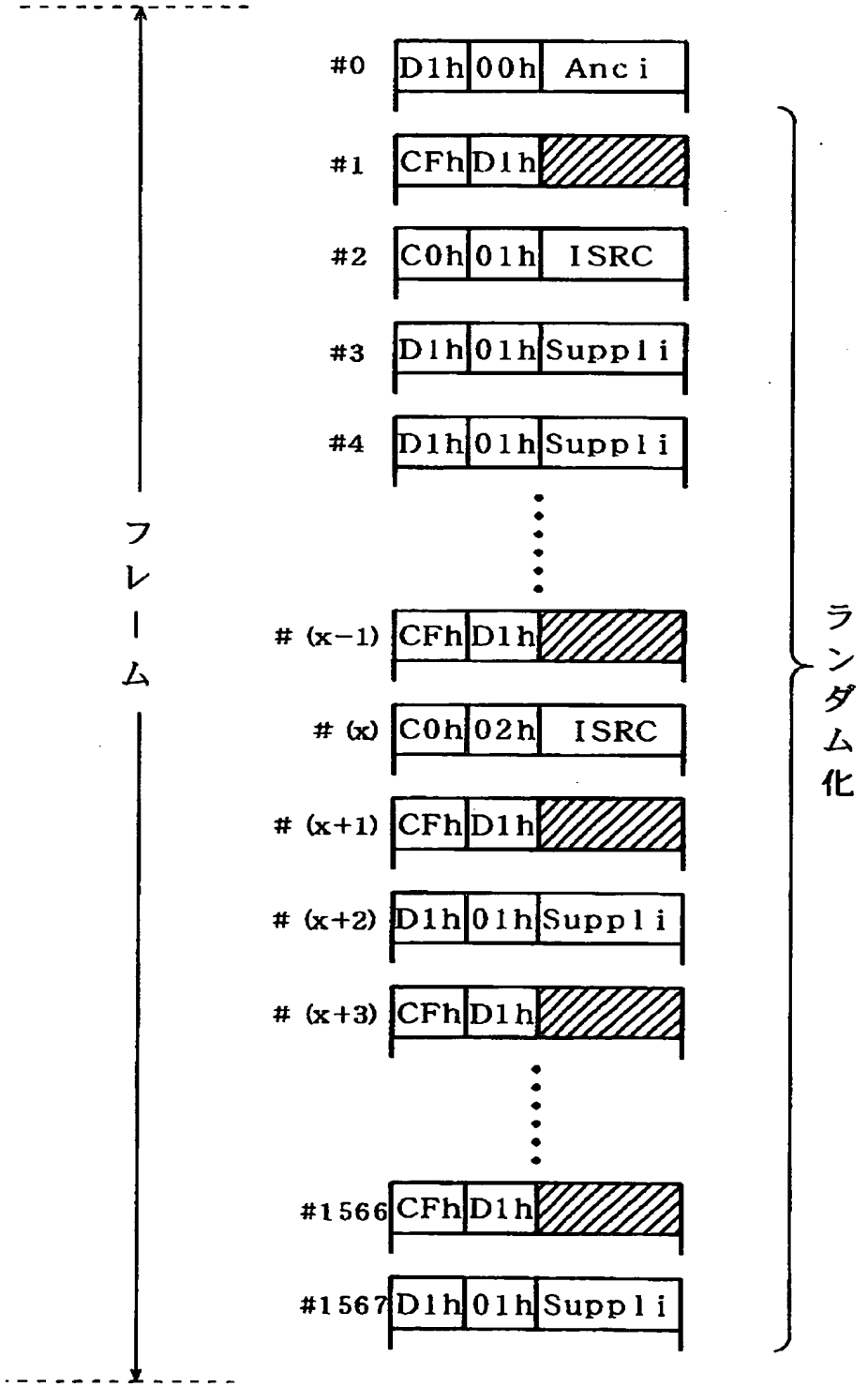
【図６】


(a)
(b)
#0 D1h 00h Anci
#1 D1h 01h Suppli
#2 D1h 01h Suppli
#3 D1h 01h Suppli
#4 D1h 01h Suppli
(x−1) D1h 01h Suppli
(x) C0h 00h ISRC
(x+1) C0h 01h ISRC
(x+2) C0h 02h ISRC
(x+3) CFh D1h
#1566 CFh D1h
#1567 CFh D1h
フレーム #M
(x) CFh D1h
(x+1) C0h 02h ISRC
(x+2) C0h 03h ISRC
(x+3) CFh D1h
#1566 CFh D1h
#1567 C0h 01h ISRC
ランダム化
通常の
ブロックシーケンス
本例の
ブロックシーケンス

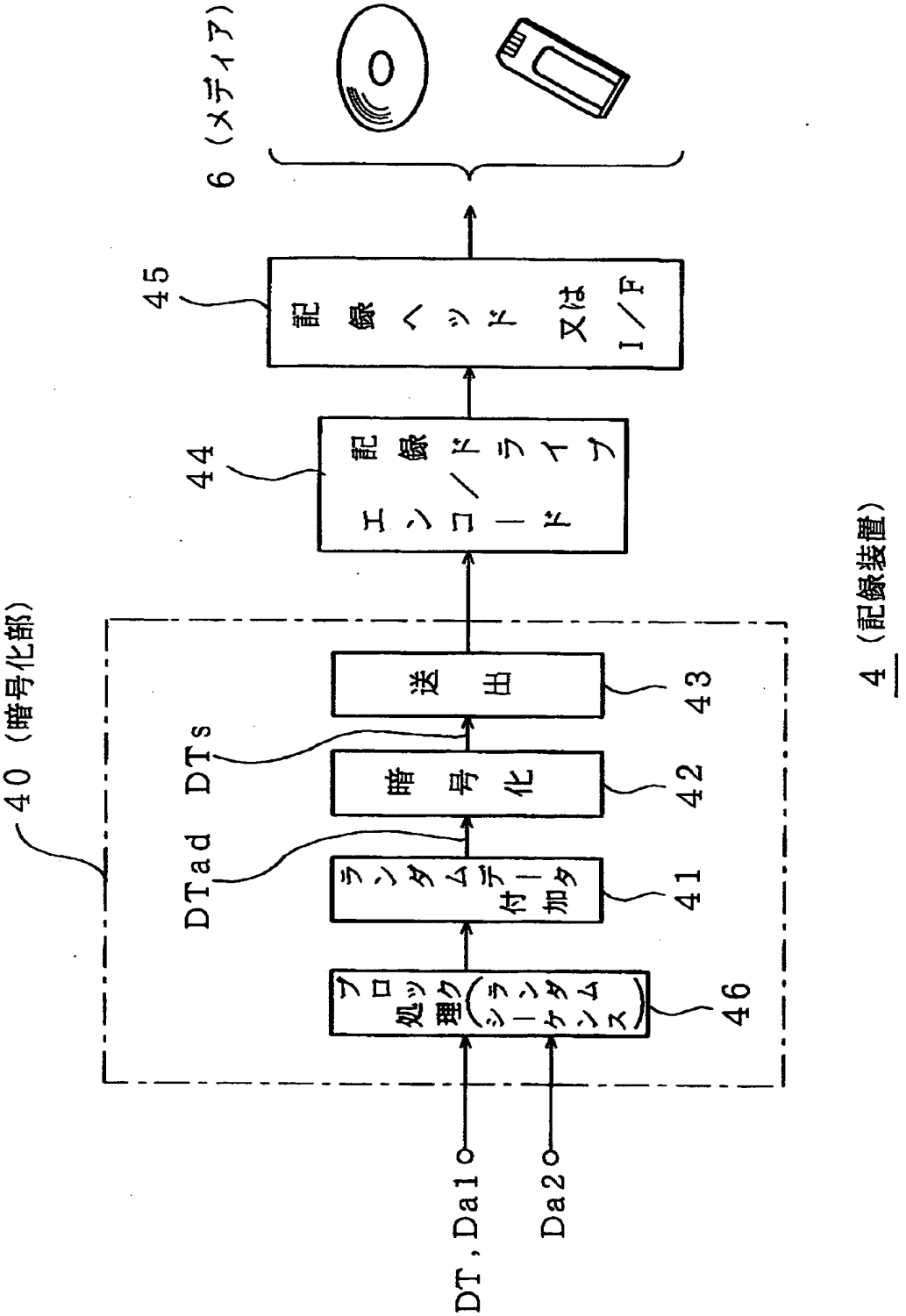
【図７】


フレーム
(M+1)
#0 D1h 00h Anci
#1 D1h 01h Suppli
#2 D1h 01h Suppli
#3 D1h 01h Suppli
#4 D1h 01h Suppli
(x−1) D1h 01h Suppli
(x) C0h 03h ISRC
(x+1) CFh D1h
(x+2) CFh D1h
(x+3) C0h 01h ISRC
#1566 C0h 02h ISRC
#1567 CFh D1h
ランダム化

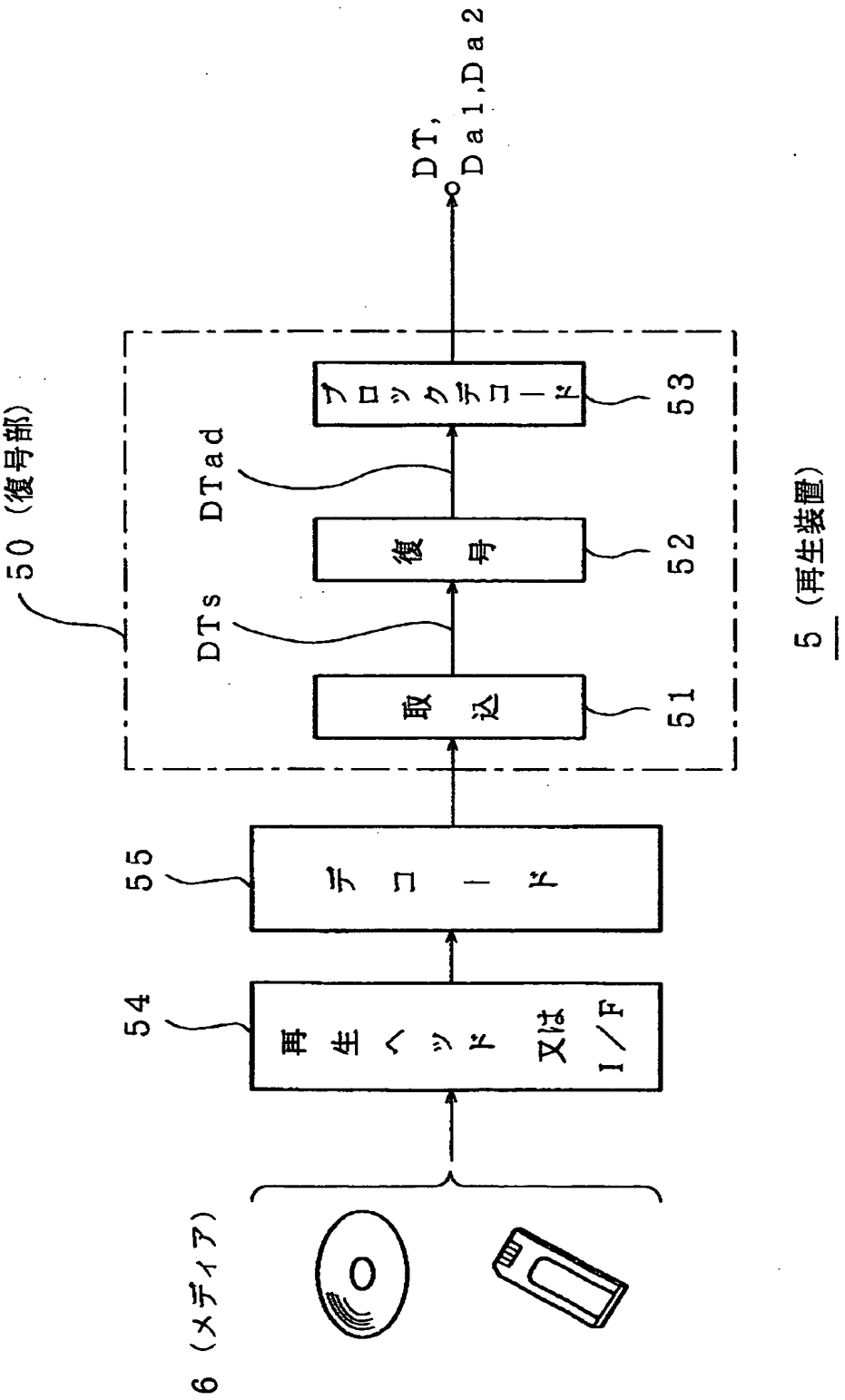
【図８】


フレーム
#0 D1h 00h Anci
#1 CFh D1h
#2 C0h 01h ISRC
#3 D1h 01h Suppli
#4 D1h 01h Suppli
(x−1) CFh D1h
(x) C0h 02h ISRC
(x+1) CFh D1h
(x+2) D1h 01h Suppli
(x+3) CFh D1h
#1566 CFh D1h
#1567 D1h 01h Suppli
ランダム化

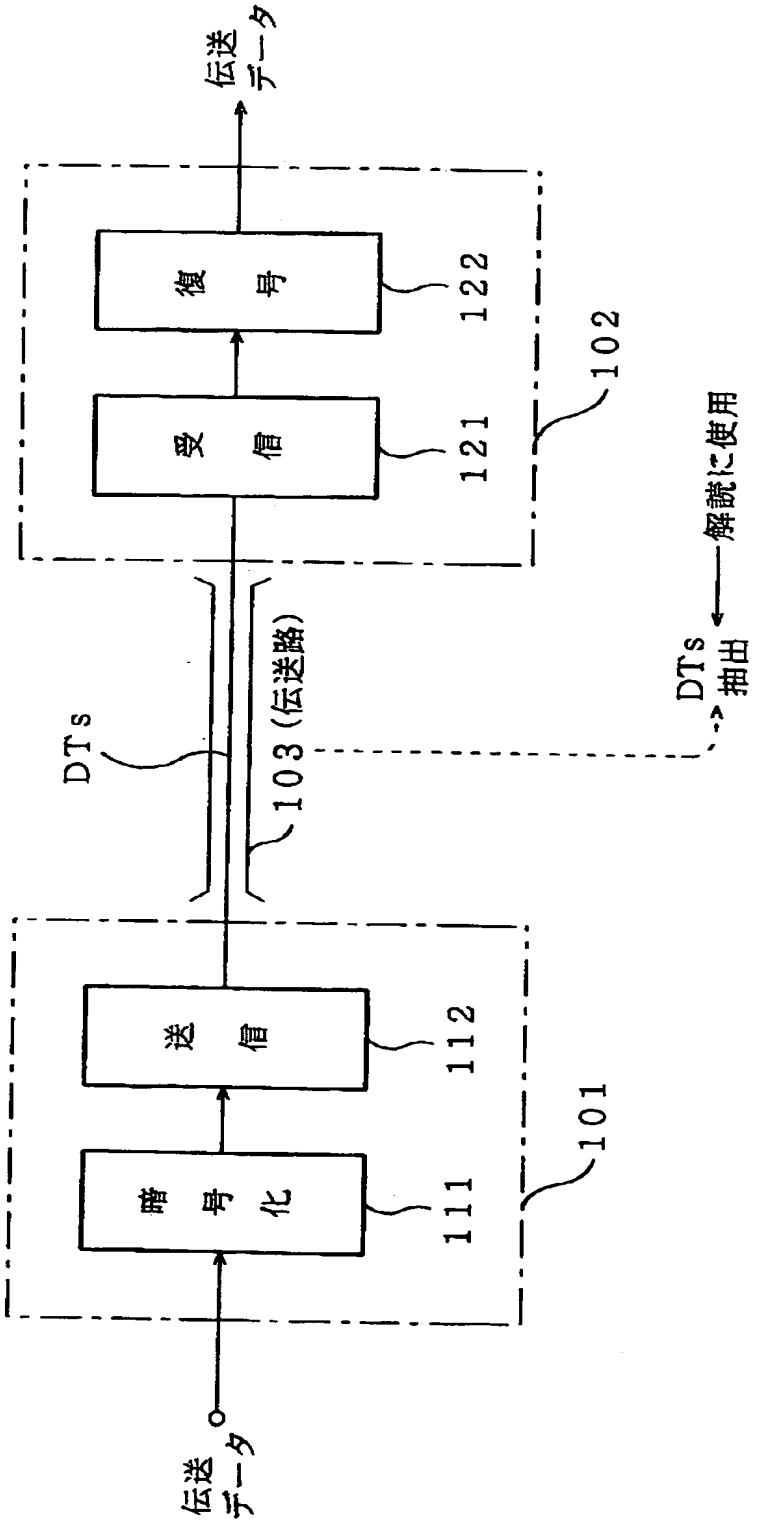
【図９】


6（メディア）
45
記録バッド又はI／F
44
記録ドライブエンコード
送出
43
暗号化
42
ランダムデータ付加
41
プロック処理（シランダムシス）
46
40（暗号化部）
DTad
DTs
DT，Da1
Da2
4（記録装置）

【図１０】


DT,
Da1,Da2
ブロックデコード
53
復号
52
取込
51
DTad
DTs
50（復号部）
5（再生装置）
デコード
55
再生バッファ又はI／F
54
6（メディア）

【図１１】


伝送データ
復号
122
受信
121
102
解読に使用
DTs
抽出
DTs
103（伝送路）
送信
112
符号化
111
101
伝送データ

【書類名】　　要約書

【要約】

【課題】　暗号解読が困難で著作権保護などに好適なデータ伝送の実現。

【解決手段】　伝送するデータとしての連続したデータブロックに対して、付加データをランダムに選択したデータブロックに付加することで、付加データが付加される位置が連続するデータブロック内でランダムなものとなるようにしている。これによって、伝送されている暗号化データにおいて、「元の内容が明白なデータ」が配されている位置がわからないようにし、暗号アルゴリズムの解読を困難にする。

【選択図】　　図６

認定・付加情報

特許出願の番号	特願２０００－２６４５０６
受付番号	５００００５０４４６０４
書類名	特許願
担当官	塩崎　博子　　１６０６
作成日	平成１２年　９月　４日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川６丁目７番３５号
【氏名又は名称】	ソニー株式会社

【代理人】　申請人

【識別番号】	100086841
【住所又は居所】	東京都中央区新川１丁目２７番８号　新川大原ビル６階
【氏名又は名称】	脇　篤夫

【代理人】

【識別番号】	100114122
【住所又は居所】	東京都中央区新川１丁目２７番８号　新川大原ビル６階　脇特許事務所
【氏名又は名称】	鈴木　伸夫

次頁無

出証特２０００－３１０６２１２

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社